Abstract of the Disclosure

Access privileges of a client are authenticated without using user account data. If an RSA modulus and public key have been assigned to the requested web page, the access privilege authentication controller 105 calls the challenge generator 107 to generate a challenge and transmits this challenge to the client 201 via the I/O controller 102. Subsequently, the access privilege authenticator 104 waits for a response from the client 201 sent via the I/O controller 102. When a response is received from the client 201, the access privilege authenticationcontroller105callstheaccessprivilegeverifier 108 to verify whether the response is correct. If the response is correct, data indicating that the access privileges have been successfully authenticated is outputted, thereby alloying the client to access the requested service.